PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: September 4, 1998

Application Number: Japanese Patent Application No. 10-251193

Applicant(s): NIPPON TELEGRAPH AND TELEPHONE CORPORATION

August 30, 1999

Commissioner,
Patent Office Takeshi Isayama (Seal)

Certificate No.11-3060041

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　９月　４日

出願番号
Application Number: 平成１０年特許願第２５１１９３号

出願人
Applicant (s): 日本電信電話株式会社

１９９９年　８月３０日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号　出証特平１１－３０６００４１

【書類名】　特許願

【整理番号】　NTTH105937

【提出日】　平成10年 9月 4日

【あて先】　特許庁長官殿

【国際特許分類】　G06C

【発明の名称】　抽出電子透かし情報統計処理方法、その装置及びプログラム記憶媒体

【請求項の数】　16

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　小川　宏

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　中村　高雄

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　富岡　淳樹

【発明者】

【住所又は居所】　東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

【氏名】　髙嶋　洋一

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【選任した代理人】

【識別番号】　100100642

【弁理士】

【氏名又は名称】　稲垣　稔

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　抽出電子透かし情報統計処理方法、その装置及びプログラム記憶媒体

【特許請求の範囲】

【請求項１】　情報コンテンツに埋め込まれた電子透かし情報を再構成する方法において、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて、情報コンテンツに埋め込まれていた電子透かし情報を再構成することを特徴とする抽出電子透かし情報統計処理方法。

【請求項２】　請求項１記載の方法において、

抽出した電子透かし情報の信頼度のしきい値を予め決めておき、

情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率を、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に基づいて計算し、

その出現確率又は１－出現確率が上記信頼度のしきい値を超えている場合のみ電子透かし情報を再構成し、超えていない場合は電子透かし無しもしくは不明と判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項３】　請求項２記載の方法において、

抽出した電子透かし情報を再構成するのに、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率から判定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項４】　請求項１乃至３の何れかに記載の方法において、

電子透かし情報とその信頼性を、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求めることを特徴とする抽出電子透かし情報統計処理方法。

【請求項５】　請求項１乃至４の何れかに記載の方法において、

電子透かし情報として実際に埋め込まれる情報系列を疑似乱数系列により予め

変調しておき、

電子透かし情報再構成処理の前に電子透かし埋め込みに用いた同じ疑似乱数系列で復調することを特徴とする抽出電子透かし情報統計処理方法。

【請求項６】　請求項５記載の方法において、

情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率を共に１／２に固定することを特徴とする抽出電子透かし情報統計処理方法。

【請求項７】　情報コンテンツに埋め込まれた電子透かし情報を再構成する装置であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する抽出手段を有することを特徴とする抽出電子透かし情報統計処理装置。

【請求項８】　請求項７記載の装置において、

上記抽出手段は、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率と電子透かし情報長から二項分布を求める手段と、

上記情報コンテンツの各ビット値に関して電子透かし系列を抽出する手段と、

上記抽出した電子透かし情報の出現確率を、上記求めた二項分布から求める手段と、

その求めた出現確率が信頼度のしきい値より大きいか否か判定する手段と、

上記しきい値より大きいと判定された情報について電子透かし情報を再構成する手段とよりなることを特徴とする抽出電子透かし情報統計処理装置。

【請求項９】　請求項８記載の装置において、

上記求めた出現確率から、上記再構成した情報ビットについての信頼度を求めて、その再構成情報ビットと共に出力する手段を備えることを特徴とする抽出電子透かし情報統計処理装置。

【請求項１０】　請求項７乃至９の何れかに記載の装置において、

電子透かし情報として実際に埋め込まれる情報系列を疑似乱数系列により予め変調する手段と、

電子透かし情報再構成処理の前に電子透かし埋め込みに用いた同じ疑似乱数系

列で復調する手段を有することを特徴とする抽出電子透かし情報統計処理装置。

【請求項１１】　情報コンテンツに埋め込まれた電子透かし情報を再構成するプログラムを格納した記憶媒体であって、

情報コンテンツから抽出された再構成前の情報系列から、統計学における二項分布に基づく検定方法を用いて情報コンテンツに埋め込まれていた電子透かし情報を再構成する処理を

コンピュータが実行することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項１２】　請求項１１記載の記憶媒体において、

抽出した電子透かし情報の信頼度のしきい値を予め決めておき、

情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率を、

情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に基づいて計算する処理と、

その計算した出現確率又は１－出現確率が信頼度のしきい値を超えている場合のみ電子透かし情報を再構成し、超えていない場合は電子透かし無しもしくは不明と判定する処理とを上記プログラムが有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項１３】　請求項１２記載の記憶媒体において、

抽出した電子透かし情報を再構成するのに、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率から判定する処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項１４】　請求項１１乃至１３の何れかに記載の記憶媒体において、

電子透かし情報とその信頼性を、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求める処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項１５】　請求項１１乃至１４の何れかに記載の記憶媒体において、

電子透かし情報として実際に埋め込まれる情報系列を疑似乱数系列により予め

変調しておき、電子透かし情報再構成処理の前に電子透かし埋め込みに用いた同じ疑似乱数系列で復調する処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【請求項１６】　請求項１５の記憶媒体において、

情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率を共に１／２に固定する処理を有することを特徴とする抽出電子透かし情報統計処理プログラム格納記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

マルチメディア著作物は、不正複製や改竄（かいざん）が容易であることから、情報利用者の正当な二次利用やコンテンツ提供者の情報発信の障害となっており、その著作権保護が訴えられている。画像や音声などのメディアの冗長性を利用し、人間に知覚されないように主情報である情報コンテンツに別の副情報を埋め込む技術に『電子透かし技術』がある。この技術は、重畳した情報の分離が困難なことより、マルチメディア著作物の著作権保護に有効な手段として考えられている。この発明は、電子透かしを用いたシステムにおける、抽出透かし情報の統計処理に関する方法及びその装置及び抽出情報の統計処理プログラムを格納した記憶媒体に関するものである。

【０００２】

【従来の技術】

特願平８－３０５３７０もしくは特願平８－３３８７６９もしくは特願平９－９８１２もしくは特願平９－１４３８８もしくは特願平９－５７５１６もしくは特願平９－１０９９２４もしくは特願平９－１６４４６６もしくは特願平９－１９７００３もしくは特願平９－２１８４６７もしくは特願平１０－３３２３９などに記載の電子透かし技術（Ｄｉｇｉｔａｌ　Ｗａｔｅｒｍａｒｋ，Ｄａｔａ　Ｈｉｄｉｎｇ，　Ｆｉｎｇｅｒ　Ｐｒｉｎｔｉｎｇ，　Ｓｔｅｇａｎｏｇｒａｐｈｙ，画像・音声深層暗号などとも呼ぶ）を用いたシステムにおいて一番重要な問題は、埋め込んだ情報の有無の判定および埋め込んだ情報の信頼性の精度であ

る。電子透かしシステムは、電子透かしを埋め込んだ情報コンテンツに対する様々なメディア処理を想定して、情報コンテンツに埋め込まれている副情報（以下電子透かし情報と呼ぶことにする）がある程度壊れていても、正しい電子透かし情報を再構成する機構を持っているものが一般的である。しかしながら現状は、再構成した透かし情報の正当性を定量評価できないものがほとんどであり、信頼性に欠けるものであった。

【０００３】

【発明が解決しようとする課題】

電子透かし情報を読みとった際に起こる問題である、電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価できる方法を、装置、プログラム記憶媒体を提供することをこの発明は目的とする。

【０００４】

【課題を解決するための手段】

電子透かし処理は、電子透かし埋め込み・電子透かし抽出の対から成る。電子透かし埋め込み処理では、秘密鍵情報などを用いて、情報コンテンツ内の電子透かし対象領域Ａから電子透かし埋め込み領域Ｂ⊆Ａを選定し、固有の規則で領域Ｂ内のデータを変更する。電子透かし抽出処理では、電子透かし埋め込み領域Ｂのデータを解釈し、電子透かし情報を再構成する。この発明では、電子透かしが埋め込まれている情報コンテンツにおいて、この発明適用対象となる電子透かしアルゴリズムを用いて、電子透かし対象領域の全体であるＡから正誤を問わず任意の秘密鍵情報を用いて読みとられる電子透かし情報の統計学における二項分布をもとに、正しい秘密鍵情報を用いて透かし埋め込み領域Ｂから読みとられた電子透かし情報がどの程度確率的に起こり得るのかを判定する。

作用

この発明によれば、電子透かし技術において、情報コンテンツから読みとった透かし情報の信頼性を定量的に評価でき、電子透かしが入っていない情報コンテンツを有りと判断したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを読みとったりする確率を一定の値で抑えることができる。

【０００５】

【発明の実施の形態】

実施例１

予め意味が曖昧な言葉の定義を行なっておく。

電子透かし系列とは、情報コンテンツから読み出された再構成処理を行なう以前の情報系列を表し、電子透かし情報とは、情報コンテンツに本当に重畳したい、システムの運用上意味ある情報、もしくは、電子透かし系列を再構成処理し得られる情報を表すものとする。

【０００６】

同様に埋め込み系列とは、実際に埋め込まれる情報を表し、埋め込み情報を変調したり、引き伸ばしたり、繰り返したりしている系列になっている。

以下にこの発明の実施例１を図面を参照して説明する。

図１は、この発明の背景となる電子透かしシステムの概要図である。

電子透かし情報１０１は、電子透かし埋め込み装置１０２によって情報コンテンツ１０３に埋め込まれ、電子透かし入り情報コンテンツ１０４に変換される。

【０００７】

電子透かし入り情報コンテンツ１０４は、無線・有線・パッケージ媒体などで流通する間に、情報圧縮やメディア処理などによって品質劣化した電子透かし入り情報コンテンツ１０５に変化する。

この発明の要部である電子透かし情報再構成装置１０６は電子透かし抽出装置１０７内部に実装され、電子透かし抽出装置１０７を用いて、劣化した電子透かし入り情報コンテンツ１０５から読みとった電子透かし系列を電子透かし情報再構成装置１０６を用いて処理し、抽出電子透かし情報１０８を抽出するという構成になる。

【０００８】

以上が電子透かし埋め込み・抽出手順の概要である。

以下、電子透かし情報再構成処理の動作を詳細に説明する。

図２は、電子透かし抽出装置１０７の内部に実装された電子透かし情報再構成装置１０６の概要である。

電子透かし情報再構成装置１０６は；電子透かし抽出装置１０７を利用して、電子透かし情報の全埋め込み対象領域から任意の１ビット電子透かし系列を抽出したときにビット１が抽出される確率ｑを予め求めておく。

【０００９】

すなわち、１ビット電子透かし系列抽出処理部２０１のようなものを仮定し、電子透かし対象領域の全要素に対して１ビットずつ電子透かし系列の抽出を行ない（破線Ｌ１）、この全試行のうちビット１が何回取り出されたかの率を計算する。

この実施例ではビット１の抽出確率および個数を求めているが、ビット０の抽出確率および個数を求めても実装上の違いのみであり、本質的に変わらないことを留意しておく。

【００１０】

これより、電子透かしアルゴリズムを用いて、情報コンテンツ１０５の電子透かし対象領域から無作為に１ビット電子透かし系列の抽出を行なったときのビット０と１の出現確率はそれぞれ１－ｑおよびｑと計算される。

ｎビット電子透かし系列抽出処理装置２０２は、電子透かしが埋め込まれている情報コンテンツから電子透かしが埋め込まれたのべ回数だけ電子透かし系列の抽出を行なう。

【００１１】

ここで、電子透かし情報を$b_0\ b_1 \cdots b_{m-1}$，$b_i \in \{0, 1\}$，$i < m$（情報長ｍビット）、ｉビット目の電子透かし情報を情報コンテンツに埋め込んだ繰り返し回数（拡散率、ｃｈｉｐ－ｒａｔｅなどとも呼ぶ）をn_i回、読みとった電子透かし系列を

$$b'_{0,0}\ b'_{0,1} \cdots b'_{0,n0-1}\ b'_{1,0}\ b'_{1,1} \cdots b'_{1,n1-1} \cdots$$
$$b'_{m-1,0}\ b'_{m-1,1} \cdots b'_{m-1,nm-1-1}$$
$$b'_{i,j} \in \{0, 1\}$$

（長さ$\Sigma_{r=0}^{m-1} n_r$ビット列）と定義する。

【００１２】

電子透かし情報再構成装置１０６は、ｎビット電子透かし情報抽出処理部２０

２から、電子透かし情報の０番目に相当する電子透かし系列の部分列からｍ－１番目に相当する電子透かし系列の部分列までを順次入力として受けとる（実線Ｌ２）。

次に、実際に電子透かし情報のｉビット目の電子透かし情報を再構成する方法を具体的に述べる。

【００１３】

電子透かし対象領域から任意にn_i ビット電子透かし系列の抽出を行なったとき、このn_i ビット列にビット１がｋ個現れる確率Ｐ（ｘ＝ｋ）は、二項分布の密度関数によって

$$P(x=k) = {}_{n_i}C_k \, q^k \cdot (1-q)^{ni-k} \qquad (1)$$

で表され、その分布関数Ｆ（ｘ）は、

$$F(x) = \sum_{k=0}^{x} {}_{n_i}C_k \, q^k \cdot (1-q)^{ni-k} \qquad (2)$$

$$(0 \leq x \leq n_i)$$

である。ただし、$_{n_i}C_k$ は、n_i 個の中からｋ個のものを選ぶ組合せ数を表す。

【００１４】

電子透かし情報の信頼度のしきい値α（１／２＜α≦１）を設け、電子透かし情報再構成装置１０６に入力された電子透かし情報のｉ番目に相当する電子透かし系列の部分列$b'_{i,0}\ b'_{i,1} \cdots b'_{i,ni-1}$に含まれるビット１の数を

$$k_i = \sum_{r=0}^{ni-1} b'_{i,r}$$

によって計算し、式（２）を用いて電子透かし情報を

$$b_i = \begin{cases} 0 & 0 \leq F(k_i) \leq 1-\alpha \text{ のとき} \\ 1 & \alpha \leq F(k_i) \leq 1 \text{ のとき} \\ \text{不明もしくは無し} & 1-\alpha < F(k_i) < \alpha \text{ のとき} \end{cases} \qquad (3)$$

と判定する。

【００１５】

見方を変えて電子透かし系列n_i に含まれるビット１の個数によって判定すると、$0 \leq F(x=x_0) \leq 1-\alpha$を満たす最大の$x_0$ と、$\alpha \leq F(x=x_1) \leq 1$を満たす最小の$x_1$ をしきい値として、図３に示すようにn_i 個中の１がx_0

以下なら０と、x_1 以上なら１と透かし情報を判定する。

図３の横軸は電子透かし系列に含まれるビット１の個数、縦軸はその出現頻度を表す。

【００１６】

電子透かしシステムによっては、情報コンテンツ１０５から抽出された電子透かし系列の分布Ｐ（ｘ）の中心値に対する偏りから再構成した電子透かし情報を求め、抽出された電子透かし系列が統計的にどの程度の確率で出現するのかを式（２）の値で求めて、再構成された電子透かし情報が１の場合は$F(k_i)$を、情報が０の場合は$1-F(k_i)$を電子透かしの信頼度として付加して出力することも可能である。この電子透かしの信頼度$F(k_i)$，$1-F(k_i)$は、情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の、情報コンテンツから任意に抽出した１ビット系列の各ビットの出現確率から得られる二項分布に対する情報コンテンツにおける抽出した再構成前の電子透かし情報の出現確率の偏りから求めたものになる。

【００１７】

この処理を電子透かし情報の情報長ｍビットに拡張した概念を図４に示す。

電子透かし情報再構成装置１０６は、再構成した電子透かし情報$b_0\ b_1 \cdots b_{m-1}$を抽出電子透かし情報１０８として出力する。

以上が電子透かし情報再構成処理の動作についてである。

この処理の手順を図５に示す。電子透かし入り情報コンテンツ１０５と、電子透かし情報抽出に必要な秘密情報が入力され、その情報コンテンツ１０５から任意に抽出した１ビット系列の各ビットの出現確率と電子透かし情報長から二項分布Ｆ（ｘ）を予め求める、つまり式（２）を求める（Ｓ１）。一方情報コンテンツ１０５と秘密情報とを用いて、各ビット値に関して、電子透かし系列を抽出する（Ｓ２）。その抽出した電子透かし情報k_iの出現確率$F(k_i)$を、予め求めておいた二項分布Ｆ（ｘ）から求める（Ｓ３）。この出現確率$F(k_i)$に対し判定式（３）を適用する。換言すると、$F(k_i)$、又は$1-F(k_i)$が信頼度のしきい値αより大きいか否かの判定を行い（Ｓ４）、しきい値αより大であれば、電子透かし情報を再構成する（Ｓ５）。つまり$F(k_i) > \alpha$であれば

、その電子透かし情報を１とし、１－Ｆ（k_i）＞αであれば電子透かし情報を０とする。このようにしてすべてのビット値に関して再構成処理を終了すると電子透かし情報を出力する。つまりステップＳ２～Ｓ５を電子透かしのビット長さだけ繰り返す。ステップＳ４でＦ（k_i）、１－Ｆ（k_i）の何れもしきい値αより大でなければ、電子透かし情報は無い、又は電子透かし情報は不明と判定して処理を終了する（Ｓ６）。

【００１８】

実施例１では、式（１）に表される分布に偏りがない、つまり、$q \simeq 1/2$となることを前提としている。

電子透かし情報のそれぞれのビット埋め込み回数n_iが、統計的特徴を得るのに十分な数である場合、一般的には、$q \simeq 1/2$となるが、ｑの値は、電子透かしアルゴリズムと情報コンテンツの特徴に依存するため、稀にｑが１／２から大きく外れた数となることがある。

【００１９】

この問題を回避する方法を実施例２で示す。

実施例２

以下にこの発明の実施例２を図面を参照して説明する。

図６は、この実施例２を付加した電子透かしシステムの概要図である。

電子透かし埋め込み装置１０２が情報コンテンツ１０３に電子透かし情報１０１を埋め込む際に、電子透かし情報の各ビット値をn_i回繰り返して埋め込む処理において、電子透かし埋め込み装置１０２の内部に実装された疑似乱数系列発生器（甲）５０１を用いて、埋め込み系列を変調し、これを情報コンテンツ１０３に埋め込む。

【００２０】

例えば、埋め込み系列を

$$b_{0,0}b_{0,1}\cdots b_{0,n0-1}b_{1,0}b_{1,1}\cdots b_{1,n1-1}\cdots b_{m-1,0}b_{m-1,1}\cdots b_{m-1,nm-1-1}$$

$$b_{i,j} \in \{0,\ 1\}$$

疑似乱数系列を

$$r_{i,0}\ r_{i,1}\cdots r_{i,ni-1}$$

$$r_{i,j} \in \{0, 1\}$$

とおくと、埋め込み系列を疑似乱数系列によって

$$m_{i,0}\ m_{i,1} \cdots m_{i,ni-1}$$

$$m_{i,j} = b_{i,j} \ (+)\ r_{i,j}$$

に変調する。Ａ（＋）ＢはＡとＢの排他的論理和を表わす。

【００２１】

この処理により、電子透かし抽出処理には、電子透かし系列埋め込みに用いたのと同じ疑似乱数系列が必要となる。

例えば、疑似乱数系列としてM系列を用いたとする。

すると、任意のM系列を用いて１ビット電子透かし系列抽出を行なったときｑ≃１／２となり、電子透かしアルゴリズムと情報コンテンツに依存することなくこの発明を適用可能となる。

【００２２】

電子透かし抽出では、電子透かし抽出装置１０７の内部に実装された疑似乱数系列発生器（乙）５０２を用いて、

$$b'_{i,j} = m_{i,j} \ (+)\ r_{i,j}$$

により復調する。

ここで、疑似乱数発生器（甲）５０１と疑似乱数発生器（乙）５０２は、同じ疑似乱数系列を発生するように実装する必要がある。

【００２３】

復調処理により得られた電子透かし系列

$$b'_{0,0}\ b'_{0,1} \cdots b'_{0,n0-1}\ b'_{1,0}\ b'_{1,1} \cdots b'_{1,n1-1} \cdots$$
$$b'_{m-1,0}\ b'_{m-1,1} \cdots b'_{m-1,nm-1-1}$$

$$b'_{i,j} \in \{0, 1\}$$

に対して、実施例１で説明した方法により電子透かし情報を再構成する。

【００２４】

読みとった電子透かし系列のビット１の出現確率ｑは、変調の有無に関わらず二項分布に近似できると考えられるため、この実施例で示した変調処理による密度関数の分布（１）への影響はない。

また、実装において、ｑ＝１／２と仮定できるため、つまりｑを求める処理（引算）を行うことなく、式（１）でｑ＝１／２として計算することにより、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、高速化が図れる。

実施例３

実施例３では、実施例１および実施例２で示した発明の例に基づき、実際に数値を示して例を説明する。ここでは電子透かし情報を１ビットとし、その埋め込み繰り返し回数ｎを１２７回とし、電子透かし情報の全埋め込み対象領域から任意の１ビット電子透かし系列を抽出したときにビット１が抽出される確率ｑを１／２とする。信頼性のしきい値αを０．９９９９９（９９．９９９％の意）とすると、図３におけるx_0は３６、x_1は９０である。すなわち、以上の条件の下でこの発明は、電子透かし情報を、電子透かし系列（ｎビット）に現れる１の個数が３６以下である場合はビット０、９０以上の場合はビット１、それ以外の場合は電子透かしが不明もしくは無しと判定する。電子透かし情報有りと判定した場合、その正当率は９９．９９９％以上を保証できる。

【００２５】

以下は実験例を示す。

実験対象画像として１２８×１２８画素の“ｌｅｎａ”画像を用い、信頼度のしきい値αを０．９９９９９９として実験を行なった。

実験１

１ビットの透かし情報“１”を秘密鍵情報“５０，０００”を用いて１２７回繰り返し埋め込み、任意の秘密鍵情報を用いて透かし系列の読みとりを行なった。図７は、秘密鍵情報に対する読みとり透かし系列のビット１の個数を示したものである。縦軸は読みとった透かし系列におけるビット１の個数、横軸は秘密鍵情報の値を表している。ただし、透かし対象領域Ａのビット１の出現頻度はｑ＝０．４９２２４７であった。正しい秘密鍵（５０，０００）を用いた場合、ビット１の個数が透かし有無の判定しきい値x_1より大きいことから、正当率９９．９９９９％で透かし情報は１であると判定でき、正しくない秘密鍵を用いた場合はすべて透かし無しもしくは不明と判定した。

実験２

７段のM系列（初期状態６４）を用いて変調した透かし系列を埋め込み、任意の秘密鍵情報と初期状態が任意のM系列を用いて実験１と同様の実験を行なった（図８）。変調を行なうことにより、実験１のデータと比較してｑの値は０．５００００に、分散は３１．００８２６５から３１．７１８７７７とほとんど変化しなかった。透かしが抽出できたのは、正しい秘密鍵情報と疑似乱数系列の組を用いたときのみであった。また、透かし対象領域Ａの半分のデータに透かし系列を埋め込んだ場合、変調なしではｑ＝０．７４１５４７であったのに対し、変調を行なうことでｑ＝０．４９９７６８という結果が得られた。

【００２６】

【発明の効果】

１．統計学における二項分布に基づき電子透かし情報を判定することに以下の効果がある。

－電子透かしが入っていない情報コンテンツを電子透かし有りと判定したり、電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価でき、その値を電子透かしの信頼度のしきい値αを用いて２（１－α）で抑えることができる。

【００２７】

２．電子透かし情報を埋め込む前に疑似乱数終りで変調することにより以下の効果がある。

－電子透かし情報の全埋め込み対象領域から任意の１ビット電子透かし系列を抽出したときにビット１が抽出される確率ｑの偏りを無くした。

－電子透かし抽出に必要な正しい電子透かしの秘密鍵情報と抽出した電子透かし系列を復調するのに必要な疑似乱数系列無しにｑの偏りから電子透かしの有無ならびにその値を検知することが困難となった。

【００２８】

－実装において、ｑ＝１／２と仮定できるため、電子透かし情報再構成処理は多数決処理と同程度の計算量となり、処理の高速化が図れる。

αは、抽出した情報の正当率の下限を示す指標であり、電子透かしシステムの内部で管理可能な情報となっている。これは、従来の電子透かしシステムに見ら

れた、抽出した電子透かし情報の正当率を利用者に提示するものより優れている点である。

【００２９】

この発明は、誤り訂正符号と併用することでさらに大きな効果が得られる。すなわち、電子透かし情報の一部のビットだけが集中して壊れているような場合、抽出した情報は、一部のビットだけが不明で、それ以外のビット情報は正当性が高い状態にあると正確に判定できる。よって壊れたビット情報のみを誤り訂正することにより、確実に正しい情報が抽出できる。

【図面の簡単な説明】

【図１】

電子透かしシステムの概要を示す図。

【図２】

図１中の電子透かし抽出装置概要を示す図。

【図３】

電子透かし情報の判定を示す図。

【図４】

電子透かし情報再構成の概念を示す図。

【図５】

電子透かし抽出処理の手順を示す図。

【図６】

この発明の第２実施例の概要を示す図。

【図７】

透かし系列読みとり結果（変調なし）を示す図。

【図８】

透かし系列読みとり結果（変調あり）を示す図。

【書類名】　図面

【図１】

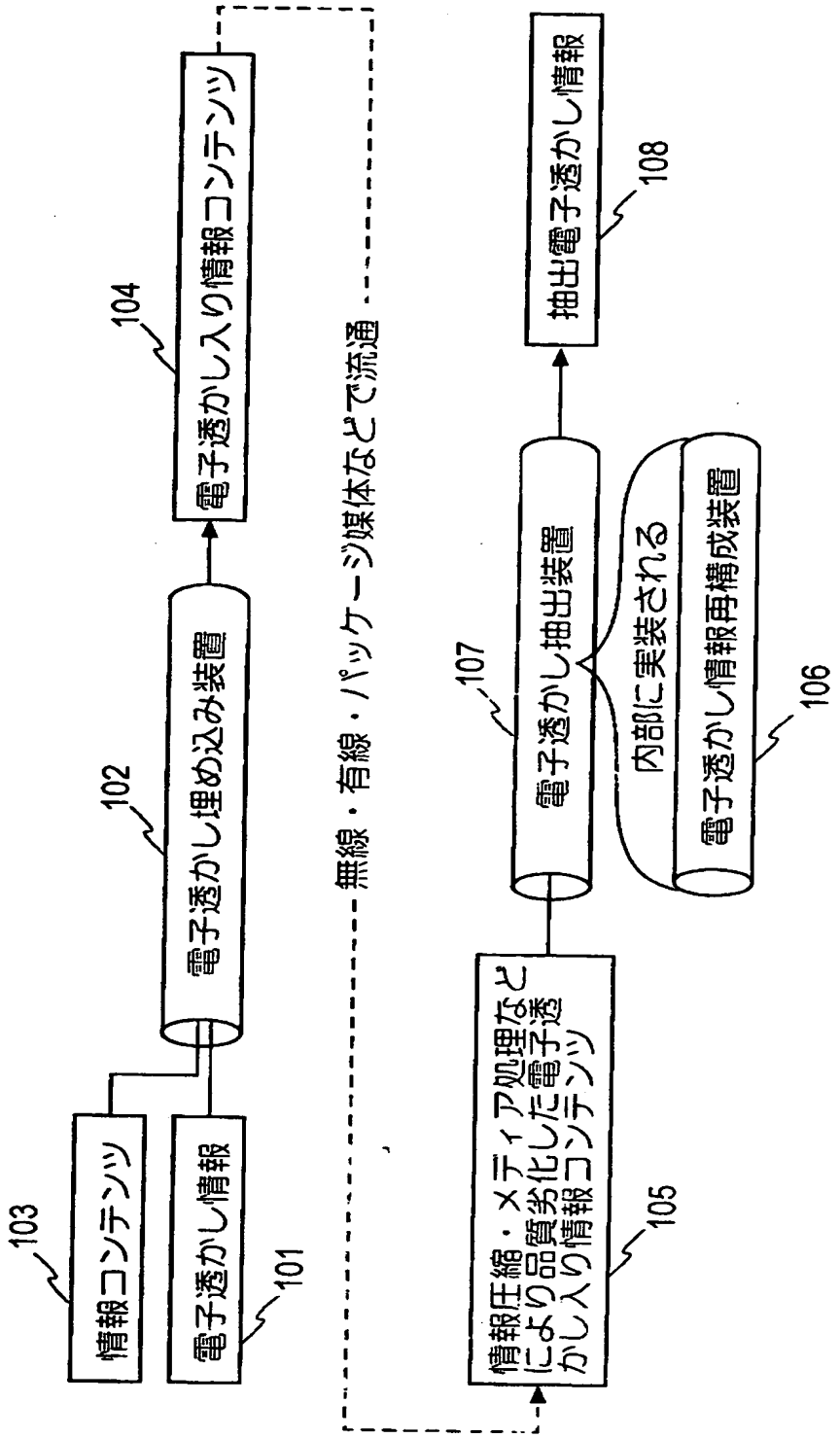
情報コンテンツ
電子透かし情報
電子透かし埋め込み装置
電子透かし入り情報コンテンツ
無線・有線・パッケージ媒体などで流通
情報圧縮・メディア処理などにより品質劣化した電子透かし入り情報コンテンツ
電子透かし抽出装置
抽出電子透かし情報
内部に実装される
電子透かし情報再構成装置
101
102
103
104
105
106
107
108

図１

【図２】

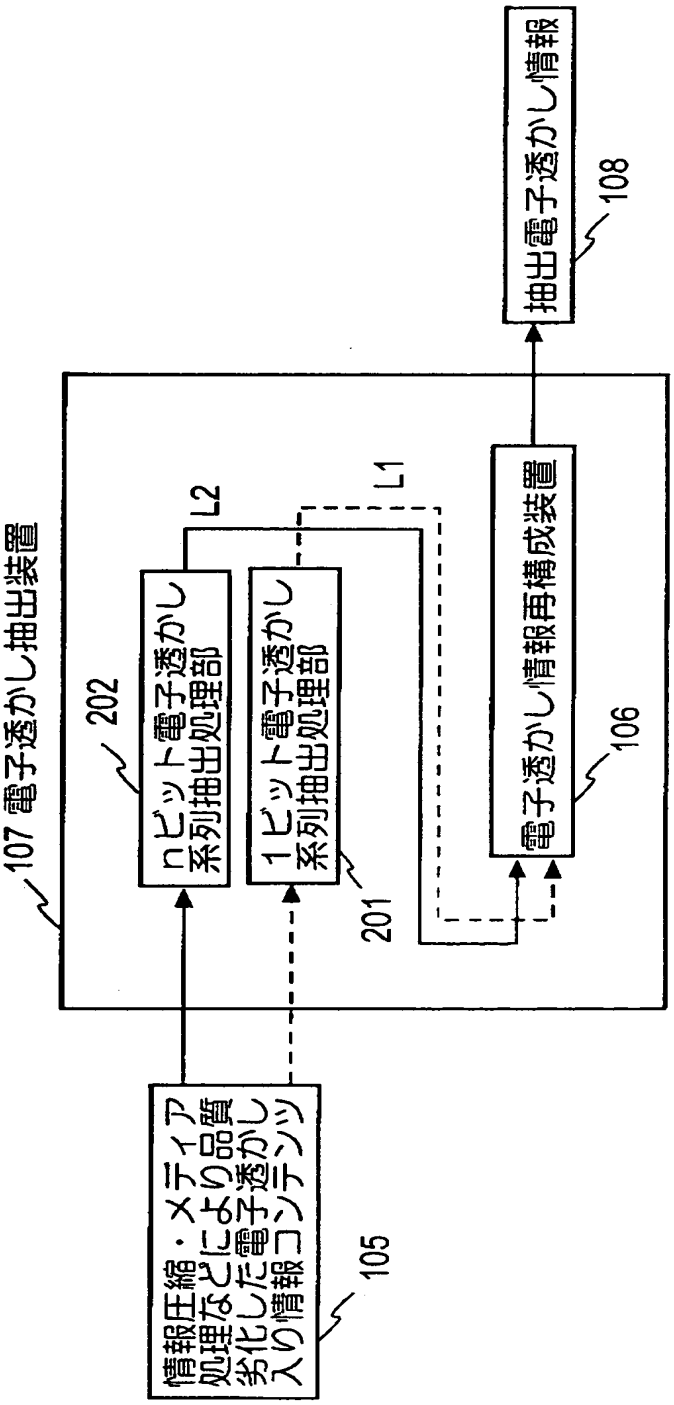
107 電子透かし抽出装置
202
nビット電子透かし系列抽出処理部
L2
1ビット電子透かし系列抽出処理部
201
L1
電子透かし情報再構成装置
106
抽出電子透かし情報
108
情報圧縮・メディア処理などにより品質劣化した電子透かし入り情報コンテンツ
105

図２

【図３】

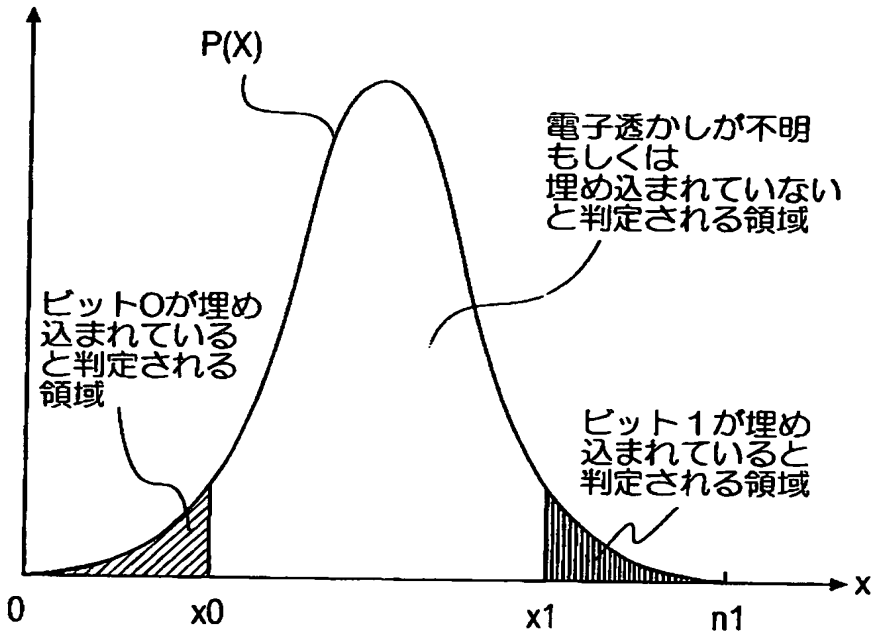
P(X)
電子透かしが不明
もしくは
埋め込まれていない
と判定される領域
ビットOが埋め
込まれている
と判定される
領域
ビット１が埋め
込まれていると
判定される領域
x
0
x0
x1
n1

図３

【図４】

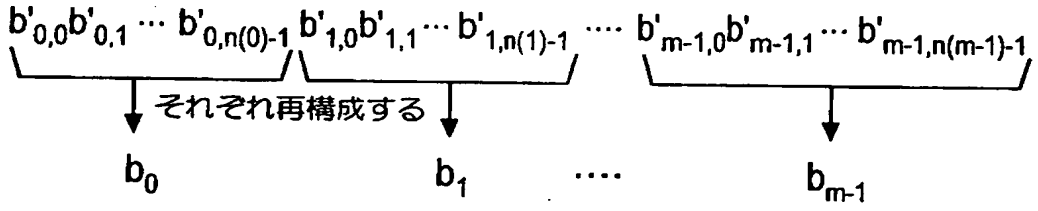
b'0,0b'0,1 … b'0,n(0)-1
b'1,0b'1,1 … b'1,n(1)-1
…
b'm-1,0b'm-1,1 … b'm-1,n(m-1)-1
それぞれ再構成する
b0
b1
…
bm-1

図４

【図５】

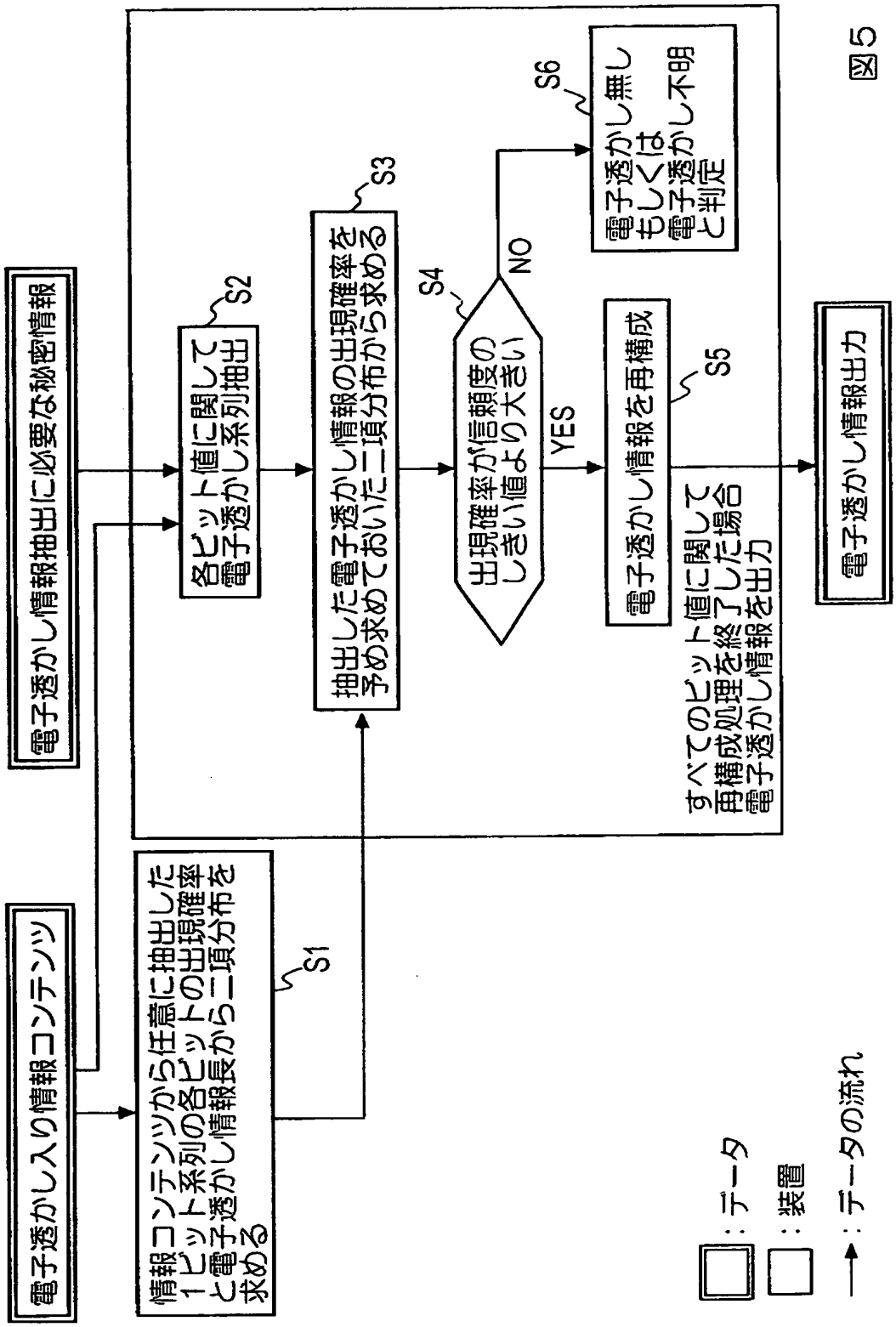
電子透かし入り情報コンテンツ
電子透かし情報抽出に必要な秘密情報
情報コンテンツから任意に抽出した1ビット系列の各ビットの出現確率と電子透かし情報長から二項分布を求める
S1
各ビット値に関して電子透かし系列抽出
S2
抽出した電子透かし情報の出現確率を予め求めておいた二項分布から求める
S3
出現確率が信頼度のしきい値より大きい
S4
NO
YES
電子透かし無しもしくは電子透かし不明と判定
S6
電子透かし情報を再構成
S5
すべてのビット値に関して再構成処理を終了した場合電子透かし情報を出力
電子透かし情報出力
：データ
：装置
：データの流れ

図５

【図６】

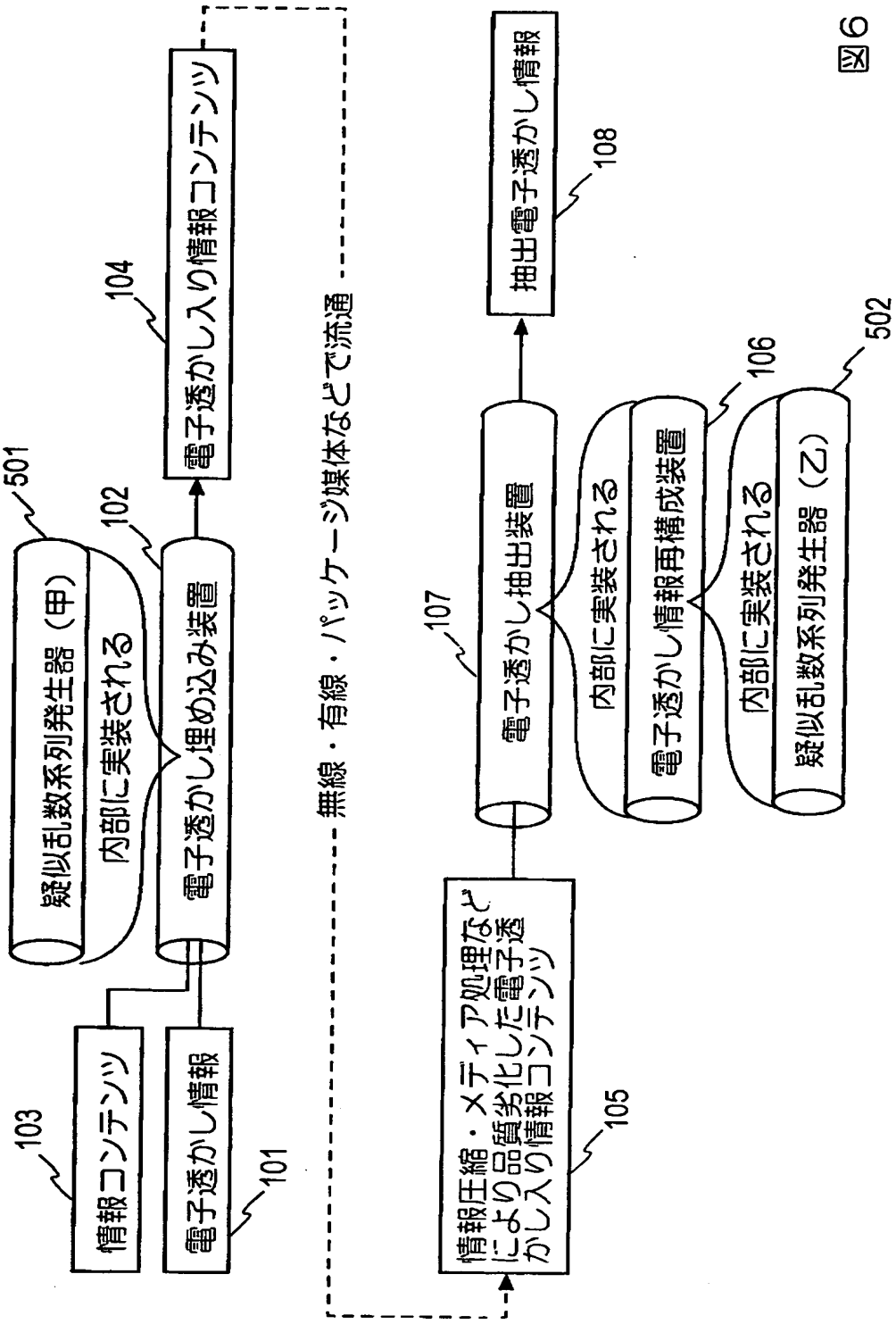
疑似乱数系列発生器（甲）
501
内部に実装される
102
電子透かし埋め込み装置
104
電子透かし入り情報コンテンツ
情報コンテンツ
103
電子透かし情報
101
無線・有線・パッケージ媒体などで流通
情報圧縮・メディア処理などにより品質劣化した電子透かし入り情報コンテンツ
105
電子透かし抽出装置
107
抽出電子透かし情報
108
内部に実装される
電子透かし情報再構成装置
106
内部に実装される
疑似乱数系列発生器（乙）
502

図６

【図７】

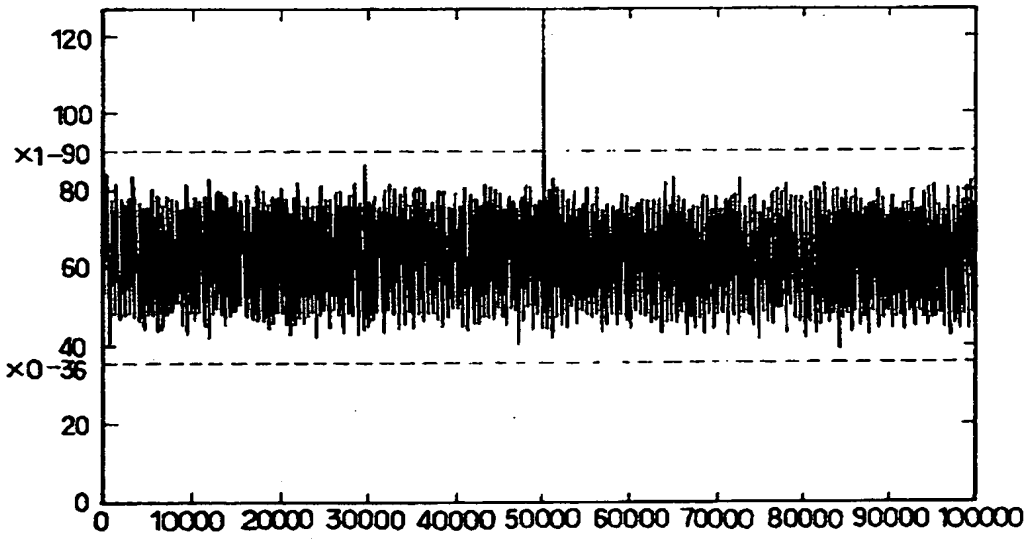
120
100
×1-90
80
60
40
×0-36
20
0
0
10000
20000
30000
40000
50000
60000
70000
80000
90000
100000

図７

【図８】

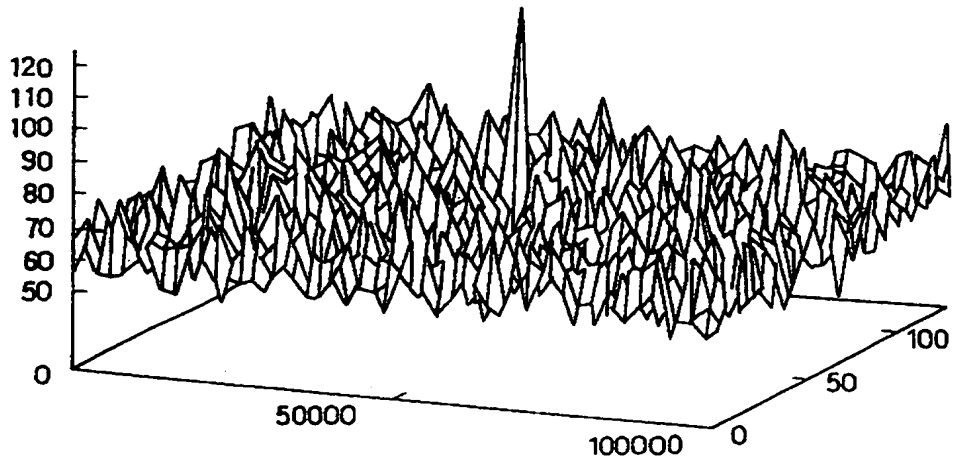
120
110
100
90
80
70
60
50
0
50000
100000
0
50
100

図８

【書類名】　　要約書

【要約】

【課題】　電子透かしが入っている情報コンテンツから正しくない電子透かしを抽出する確率を定量的に評価する。

【解決手段】　情報コンテンツの透かし対象領域から無作為に１ビット透かし系列の抽出を行い、その時のビット０と１の出現確率１－ｑとｑを求め、透かしが埋め込まれたのべ回数n_iビットだけ透かし系列を抽出し、この時、n_iビット列に１がｋ個現れる確率

$$P(x=k)={}_{n_i}C_k\, q^k \cdot (1-q)^{ni-k}$$

その分布関数

$$F(x)=\sum_{k=0}^{x} {}_{n_i}C_k\, q^k \cdot (1-q)^{ni-k} \quad (0\leq x\leq n_i)$$

より、透かし情報の信頼度のしきい値α（１／２＜α≦１）に対し、$0\leq F(x=x_0)\leq 1-\alpha$を満す最大の$x_0$と、$\alpha\leq F(x=x_1)\leq 1$を満す最小の$x_1$をそれぞれ透かし情報判定しきい値とする。

【選択図】　　図３

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000004226
【住所又は居所】　東京都新宿区西新宿三丁目１９番２号
【氏名又は名称】　日本電信電話株式会社
【代理人】　申請人
【識別番号】　100066153
【住所又は居所】　東京都新宿区新宿四丁目２番２１号　相模ビル
【氏名又は名称】　草野　卓
【選任した代理人】
【識別番号】　100100642
【住所又は居所】　東京都新宿区新宿４丁目２番２１号　相模ビル　草野特許事務所
【氏名又は名称】　稲垣　稔

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９５年　９月２１日
［変更理由］　住所変更
住　所　東京都新宿区西新宿三丁目１９番２号
氏　名　日本電信電話株式会社

２．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社